REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claims 1-24 are pending in this application. Claims 1-24 were rejected under 35 U.S.C. § 103(a) as unpatentable over "Bluetooth Specification", Bluetooth Security, November 29, 1999, pages 149-178 (herein "Bluetooth") in view of "5C Digital Transmission Content Protection White Paper" Revision 1.0, July 14, 1998, pages 1-13 (herein "5C White Paper").

Addressing the above-noted rejection, that rejection is traversed by the present response.

The claims are amended to clarify features recited therein. Specifically, independent claim 1 now further recites:

> wherein at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful.

That subject matter is fully supported by the original specification for example at page 23, lines 2-14 and Figure 6, steps S37, S38. The other independent claims are similarly amended.

Applicants respectfully submit the claims as currently written distinguish over the applied art as the claims recite specific operations of how first and second encryption keys are utilized to transmit copy protected contents data securely, and such specific combined usage of the first and second encryption keys is not taught or suggested by the combination of teachings in the Bluetooth reference and the 5C White Paper.

One objective of the present invention is to provide enhanced transfer of copyright protected contents data, and to particularly realize a secure copyright protection even in a radio network environment.[1]

With reference to Fig. 1 in the present specification as a non-limiting example, the present invention can be applied to a radio communication system including a portable MPEG4 player 101 and a portable viewer 102, which are both owned by the same person and thus that are authorized to communicate information with each other. The portable MPEG4 player 101 and the portable viewer 102 are located within an area in which a connection by a local area radio network is possible. Further, another portable viewer 103 owned by a different entity may also enter that local area, but the claimed system prevents that other portable viewer 103 from viewing data from the portable MPEG4 player 101 as the other portable viewer 103 is owned by a different entity and does not have authorization to view data provided from the portable MPEG4 player 101.

As shown for example in Figure 5 in the present specification at steps S1-S19, a first authentication is carried out to determine whether two devices can properly communicate with each other, such as devices 101 and 102 in Figure 1 in the present specification (steps S1-S16). When it is determined that those two devices can communicate with each other a first encryption key is shared between the two devices (steps S18-S19). That shared first encryption key is then utilized in a second authentication operation (in steps S21-S23).

Thereby, in the claimed invention the second authentication unit carries out a second authentication with the receiving device for protecting copyright of the contents data to be transmitted through an encrypted radio communication using the first authentication key.

With such a claimed structure, even if a receiving device in the claimed invention does not have a copyright protection function, the receiving device can communicate with a

[1] See for example the present specification at page 3, lines 3-6.

transmitting device because the second authentication is carried out after the first authentication is carried out. If the second authentication was carried out before the first authentication was carried out the receiving device would not be able to communicate with a transmitting device.

As noted above, in the claimed invention a first authentication is carried out to determine whether two devices can properly communicate with each other, and then a second authentication can be carried out. As a non-limiting example that first authentication can be a Bluetooth encryption and the second authentication can be the DTCP authentication. Thereby, in the claims, when the Bluetooth authentication and key exchange is unsuccessful, then that second DTCP authentication is rejected.

Moreover, and as now further clarified in claim 1, at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful. The other independent claims recite similar features.

Again with reference to Figure 1 in the present specification as a non-limiting example, the second authentication unit and the second key exchange unit 16 of the portable MPEG4 player (a transmitting device) 101 or the second authentication unit and second key exchange unit 26 of the portable viewer 103 (a receiving device) rejects its authentication and key exchange with the portable viewer 103 or the portable MPEG4 player 101 when the first authentication and first key exchange is unsuccessful.

As a non-limiting example the second authentication unit and second key exchange may be a Digital Transmission Contents Protection (DTCP) and the first authentication and first key exchange may be a Bluetooth authentication and key exchange.

In that non-limiting example, the DTCP authentication and key exchange unit 16 of the portable MPEG4 player 101 or the DTCP authentication and key exchange unit 26 of the portable viewer 103 rejects its process of DTCP authentication and key exchange with a portable viewer 103 or the portable MPEG4 play 101 when the Bluetooth encryption cannot be realized. That is, if Bluetooth authentication and key exchange by the Bluetooth authentication and key exchange processing unit 13 with the portable viewer 103 or the portable MPEG4 play 101 is unsuccessful, then the DTCP authentication and key exchange is rejected.

Also, the second authentication unit and the second key exchange unit are located in an upper layer (e.g., DTCP layer) relative to a layer in which the first authentication and the first key exchange (e.g., Bluetooth layer) are carried out. Therefore, the DTCP authentication and key exchange unit controls sharing the encryption key and the DTCP layer based on a result of a security level in a lower layer than the DTCP layer.

The above-noted features reflected in the claims are believed to clearly distinguish over the applied art. That is, neither the Bluetooth reference nor the 5C White Paper discloses or suggests the above-noted feature of claim 1, and the similar feature in the other independent claims, that:

> wherein at least one of the second authentication unit and the second key exchange unit rejects its process of at least one of authentication and key exchange with the receiving device when at least one of the first authentication by the first authentication unit and the first key exchange by the first key exchange unit with the receiving device is unsuccessful.

The outstanding rejection relies on the Bluetooth reference to disclose a Bluetooth authentication and key exchange and relies on the 5C White Paper to disclose a second authentication and key exchange. However, clearly the 5C White Paper does not disclose or suggest rejecting its process if at least one of a first authentication by a first authentication

unit and a first key exchange by a first key exchange unit with a receiving device is unsuccessful. The Bluetooth reference also does not provide any such teachings.

Thereby, the claims as written positively recite features that distinguish over the applied art.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)
SNS/rac
I:\ATTY\SNS\21'S\213200\213200US-AM1.DOC